UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/977,192	10/16/2001	Stefan Andersson	027557-071	3198

42015 7590 08/05/2005

POTOMAC PATENT GROUP, PLLC
P. O. BOX 270
FREDERICKSBURG, VA 22404

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/977,192	ANDERSSON, STEFAN	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/25/02, 8/22/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 1 – 50 are pending.

Election/Restrictions

Applicant's election with traverse of Group II in the reply filed on 6/16/05 is acknowledged. The Office has found the applicant's reason for traversal to be persuasive. After reconsideration of the pending claims, the Office has withdrawn the restriction.

Claim Objections

Claim 48 is objected to because of the following informalities: Nonsensical phrasing – "requested function cryptographic function". Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 7, 10 – 12, 14, 18, and 19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding these claims 7, 10 – 12, 14, and 18, they are directed to a device of which the claim language "comprising a cryptographic module" allows the device to be implemented solely in software (Specification, page 5). It is therefore rejected under 35 U.S.C. 101 as not being tangible.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 4, 6, 19, 20, 24, 26 – 28, 31 – 34, 47, and 48 are rejected under 35 U.S.C. 102(b) as being anticipated by Caputo et al., "Pocket Encrypting and Authenticating Communications Device", U.S. Patent 5,778,071.

Regarding claim 1, Caputo et al. discloses a method of authenticating communications, the method comprising:

using a mobile communications device, which includes a cryptographic module for use in mobile communication, as an cryptographic service provider (Caputo et al., Col. 2, lines 23-27; Col. 3, lines 33-38).

Regarding claim 4, Caputo et al. discloses:

providing a wired connection between the mobile communications device and the computer (Caputo et al., Col. 6, lines 41-61).

Regarding claim 6, Caputo et al. discloses:

when the application program interface requires cryptographic functionality, calling a cryptographic service provider function in the mobile communications device (Caputo et al., Col. 15, lines 13-39).

Regarding claim 19, Caputo et al. discloses:

a module for a personal computer, wherein, in response to the module receiving a first command from a cryptographic application program interface, indicating that it requires cryptographic functionality, the module sends a second command to a mobile communication device, such that the mobile communications device acts as a cryptographic service provider for said personal computer (Caputo et al., Col. 15, lines 13-39). Caputo discloses an application program running on a computer. A set of

codes and signals are issued, when encryption is requested by the application program ("a first command"), and they are sent to the device ("a second command").

Regarding claim 20, it comprises the limitations of claim 1, and is rejected for the same reasons.

Regarding claim 24, Caputo et al. discloses:

a computer; and mobile communications device, including a cryptographic module, the computer having at least one application which requires cryptographic functionality, a first part of the required cryptographic functionality being provided in the computer, and a second part of the required cryptographic functionality being provided in the mobile communications device (Caputo et al., Col. 15, lines 13-39, col. 9, lines 28-36). As disclosed, the computer provides a first part of the cryptographic functionality by providing the instructions for the encrypting device. The device provides a second part of the cryptographic functionality by executing the encryption algorithm.

the computer and the mobile communications device having means for establishing a secure communications path therebetween (Caputo et al., fig. 3); *and the computer further comprising an interface device which, on determining that an application needs use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends command thereto* (Caputo et al., Col. 15, lines 13-39).

Regarding claim 26, Caputo et al. discloses:

wherein the computer application which requires cryptographic functionality is an internal memory access application (Caputo et al., Col. 15, lines 13-39).

Regarding claim 27, Caputo et al. discloses:

wherein the computer application which requires cryptographic functionality is an external communication application (Caputo et al., Col. 15, lines 13-39).

Regarding claims 28 and 31, they are similar in limitations to claims 1 and 6, and are rejected for the same reasons.

Regarding claims 32 and 33, Caputo et al. discloses:

using a cryptographic module realized in hardware in the mobile communications device and *using a cryptographic module realized in software in the mobile communications device* (Caputo et al., Col. 9, lines 40-45).

Regarding claims 34, Caputo et al. discloses:

using a cryptographic module provided on an external smart card which can be read by the mobile communications device (Caputo et. al., Col. 10, lines 19-31, 51-59; Col. 13, lines 4-10, 25-67).

Regarding claim 47, Caputo et al. discloses:

an application interface for connection to a computer application; and an external interface for connection to a mobile communication device containing a cryptographic module wherein, when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom (Caputo et al., Col. 15, lines 13-39, figs. 3, 4a, 5a).

Regarding claim 48, Caputo et al. discloses:

wherein the module has some cryptographic functionality, and comprises means for determining in response to a request from the application interface whether it is able to provide the requested function cryptographic function (Caputo et al., Col. 15, lines 13-39). Caputo et al. discloses that the computer receives a command to have data sent to the device, encrypted, and sent to the network, or have data sent to the device, encrypted, and returned to the application interface. In response to the selected option, the computer understands the request and appropriately controls the device. Thus, it comprises means to determine that it is able to provide the requested cryptographic function.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 3, 7, 10 – 18, 21, 22, 25, 29, 30, 35 – 40, 42, and 44, are rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo et al. as applied to claims 1, 4, 6, 19, 20, 24, 26 – 28, 31 – 34, 47, and 48 above, further in view of Grimm et al., "Portable Computer Stored Removable Mobile Telephone", U.S. Patent 5,907,815, and further in view of Geiger et al., "Secure Wireless Electronic-Commerce System with Wireless Network Domain", U.S. Patent 6,463,534 B1.

Caputo et al. discloses a mobile communications device, comprising a cryptographic module, which is used as a token for authenticating a user and for encrypting communications (Caputo et al., Col. 2, lines 23-27; Col. 3, lines 33-38, 46-50; Fig. 2). The device sends communications to a recipient by wired telephonic means (Caputo et al., Fig. 2, elem. 14; Col. 16, lines 40-45; Col. 17, lines 3-7). Caputo et al, however, does not disclose that the device sends the communications by wireless means, or that the device is enabled to use the enhanced wireless security of the Wireless Application Protocol.

Grimm et al. discloses a mobile communications device ("wireless phone") that is enabled to send communications from a user of a connected computer via wireless telephonic means (Grimm et al., Col. 12, lines 12-33; Fig. 7; Fig. 9).

Thus it would have been obvious to one of ordinary skill in the art to combine the wireless mobile communication feature of Grimm et al. with the mobile communication

device of Caputo et al. because it is apparent that the ability to operate wirelessly would enhance a communication device designed to be mobile and portable.

Geiger et al., discloses a wireless mobile device and system used to send secure wireless communication using the Wireless Application Protocol (Geiger et al., Col. 2, lines 49-65; Col. 9, lines 22-53; col. 11, line 64 – col. 12, line 8). As disclosed by Geiger et al., WAP (utilizing WTLS and a WIM) is a convenient protocol to use with wireless mobile communications, chosen for its security.

Thus, it would have been obvious to one of ordinary skill in the art to employ the secure Wireless Application Protocol feature of Geiger et al. with the combination of Caputo et. al. and Grimm et al. because it is obvious that a wireless mobile communication device designed for authenticated and encrypted communications would be enhanced by the use of a convenient communication protocol and system that features increased wireless security.

Regarding claim 2, the combination of Caputo et al., Grimm et al., and Geiger et al., disclose:

the mobile communications device is a WAP-enabled device (Geiger et al., Fig. 1, Col. 9, lines 22-53). As disclosed, the device is WAP-enabled since it communicates using the WAP protocol.

Regarding claim 3, the combination of Caputo et al., Grimm et al., and Geiger et al., disclose:

wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications (Geiger et al., Col. 2, lines 49-65; Col. 6, lines 55-58; Col. 9, lines 22-53). As disclosed, communication security, the functionality provided by the cryptographic module, is accomplished using WTLS communications.

Regarding claim 7, the combination of Caputo et al., Grimm et al., and Geiger et al., disclose:

a cryptographic module, the cryptographic module being usable: for encoding wireless communications from the device; in a cryptographic service provider with an application program interface of a remote computer (Caputo et al., Col. 2, lines 23-27; Col. 3, lines 33-38, 46-50; Col. 15, lines 13-39, figs. 2, 3, 4a, 5a; Grimm et al.).

Regarding claim 10, it is substantially similar to claim 3, and is rejected for the same reasons.

Regarding claim 11, the combination of Caputo et al., Grimm et al., and Geiger et al., disclose:

wherein the cryptographic module uses public key cryptography (Caputo et al., Col. 1, lines 27-39; Col. 11, lines 18-59).

Regarding claim 12, the combination of Caputo et al., Grimm et al., and Geiger et al., disclose:

means for sending and transmitting data using WAP (Geiger et al., Fig. 1, Col. 9, lines 22-53).

Regarding claims 13, 14, and 15, they are substantially similar to claims 32, 33, and 34 and they are rejected for the same reasons.

Regarding claims 16 and 17, the combination of Caputo et al., Grimm et al., and Geiger et al., disclose:

wherein the cryptographic module comprises a Wireless Identity Module card and *wherein the cryptographic module comprises a Wireless Identity Module card which allows communications using Wireless Transport Layer Security.* (Geiger et al., col. 11, line 64 – col. 12, line 8; fig. 4, elems. 450, 452).

Regarding claim 18, the combination of Caputo et al., Grimm et al., and Geiger et al., disclose:

an interface for receiving a command from a personal computer, the mobile communications device acting as a cryptographic service provider for said personal computer in response to said command (Caputo et al., Col. 15, lines 13-39).

Regarding claims 21, 22, 25, 29, and 30, they are substantially similar to claims 2 and 3, and they are rejected for the same reasons.

Regarding claim 35, it is substantially similar to claims 16, and is rejected for the same reasons.

Regarding claim 36, the combination of Caputo et al., Grimm et al., and Geiger et al., disclose:

a cryptographic application program interface; and a cryptography service provider, wherein, when the cryptographic application program interface determines that the application requires cryptographic functionality, sends a command to the cryptography service provider (Caputo et al., Col. 15, lines 13-39), *and wherein the cryptography service provider has a communications link to a cryptographic module of a mobile communications device, the cryptographic module of the mobile communications device being usable to encrypt communications between the mobile communications device and a telecommunications network over a wireless interface* (Caputo et al., fig. 3: Grimm et al.), *and wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device* (Caputo et al., Col. 2, lines 23-27; Col. 3, lines 33-38).

Regarding claims 37, 38, 39 and 40, they are substantially similar to claims 32, 33, 34, and 35 and they are rejected for the same reasons.

Regarding claims 42, it is substantially similar to claim 48 and it is rejected for the same reasons.

Regarding claim 44, the combination of Caputo et al., Grimm et al., and Geiger et al., disclose:

the mobile communications device being able to communicate over a first wireless interface with a telecommunications network, and comprising a cryptographic module to provide cryptographic functionality for use in communications over the first wireless interface (Caputo et al., fig. 3; Grimm et al.), *the mobile communications device further comprising a security manager module for receiving commands from a computer system over a second interface, wherein, in response to suitable commands received from the computer system over the second interface, the security manager module requests a cryptographic function from the cryptographic module, and returns the results of the cryptographic function to the computer system over the second interface* (Caputo et al., Col. 15, lines 13-39).

Claims 5, 8, 9, 23, 41, 46, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Caputo et al., Grimm et al., and Geiger et al. as applied to claims 2, 3, 7, 10 – 18, 21, 22, 25, 29, 30, 35 – 40, 42, and

44 above, further in view of Ericsson, "Bluetooth – A Global Specification for Wireless Connectivity".

Regarding claims 5, 8, 9, 23, 41, 46, and 49, the combination of Caputo et al., Grimm et al., and Geiger et al. disclose a wired connection between the device and the computer (Caputo et al., Col. 6, lines 41-61). They do not disclose a wireless connection or connection via a short-range transceiver incorporating Bluetooth wireless technology.

Ericsson discloses the obvious use of wireless connections between devices (Ericsson, Page 1). Bluetooth, a short-range radio technology allows for the replacement of wired connections – "facilitating protected" wireless connections between mobile devices. As disclosed, Bluetooth technology can be used to replace "the cumbersome cable used today to connect a laptop to a cellular telephone".

It would be obvious to one of ordinary skill in the art to combine the secure feature of wireless short-range radio connection and Bluetooth technology of Ericsson with the combination of Caputo et al., Grimm et al., and Geiger et al. because it is apparent that the ability to securely operate wirelessly would enhance a security/communication device designed to be mobile and portable.

Claims 43, 45, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Caputo et al., Grimm et al., and Geiger et al. as applied to claims 2, 3, 7, 10 – 18, 21, 22, 25, 29, 30, 35 – 40, 42, and 44 above,

further in view of RSA, "PKCS #11 v2.10: Cryptographic Token Interface Standard".

Regarding claims 43, 45, and 50, the combination of Caputo et al., Grimm et al., and Geiger et al. discloses a portable encryption and authentication device. The device utilizes a modem and "industry compatible" modem commands for communication (Caputo et al., fig. 2, elem. 160; col. 17, lines 12-35). The combination, however, does not disclose specifically that the mobile communications device utilizes PKCS #11 with AT commands.

RSA discloses that the PKCS #11 command set is the industry standard for encryption and authentication devices (RSA, pages 1-12).

It would have been obvious to one of ordinary skill in the art to employ PKCS #11 command set, disclosed by RSA to be the industry standard, in the combination of Caputo et al., Grimm et al., and Geiger et al. This would have been obvious because one of ordinary skill in the art would have been motivated for the purpose of utility and compatibility to utilize the standards defined by industry. Furthermore, the disclosure of AT commands is obvious as these are the standard industry commands used to communicate via modems, as evidenced by the definitions of "AT Command Set" and "Modem Standards" in Newton's Telecom Dictionary, 13th ed.

Conclusion

Claims 1 – 50 have been rejected.

The following prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Barlow et al., "System and Method for Configuring and Managing Resources on a Multi-purpose Integrated Circuit Card Using a Personal Computer", U.S. Patent 6,038,551.

Di Santo et al., "Stand-Alone Telecommunications Security Device", U.S. Patent 6,430,691 B1.

Ganesan et al., "Modem Compatible Method and Apparatus for Encrypting Data That is Transparent to Software Applications", U.S. Patent 5,978,481.

Seiderman, "Portable Cellular Telephone With Credit Card Debit System", U.S. Patent 5,850,599.

Wang, "Portable Electronic Authorization Devices and Methods Therefor", U.S. Patent 5,917,913.

Muftic, "Smart Token System for Secure Electronic Transactions and Identification", U.S. Patent 5,943,423.

Muftic, "Secure World Wide Electronic Commerce Over an Open Network", U.S. Patent 5,850,442.

"WAP White Paper", AU-System, February 1999.

Newton, Newton's Telecom Dictionary, 13th ed., 1998.

A shortened statutory period for reply is set to expire **3** months (not less than 90 days) from the mailing date of this communication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are,unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
Assistant Examiner
Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER